On existence of nontrivial unbiased tests in quantum hypothesis testing (Theory and application of statistical inference in quantum theory)

AUTHOR(S):

Tanaka, Fuyuhiko

CITATION:

Tanaka, Fuyuhiko. On existence of nontrivial unbiased tests in quantum hypothesis testing (Theory and application of statistical inference in quantum theory). 数理解析研究所講究録 2013, 1834: 56-67

ISSUE DATE:

2013-05

URL:

http://hdl.handle.net/2433/194884

数理解析研究所講究録
第1834巻 2013年 56-67

On existence of nontrivial unbiased tests in quantum hypothesis testing

東京大学・情報理工学系研究科　田中冬彦
Fuyuhiko Tanaka
Graduate School of Information Science and Technology,
The University of Tokyo

Abstract

Recently, there have lots of work in quantum hypothesis testing that lies in the core of fascinating applications in quantum information theory. They mainly deal with a simple hypothesis because their main concern is the distinguishability of two quantum states. However, in a practical application, composite hypothesis testing is much important as in classical statistics. In the present paper, we focus on the unbiased test in the quantum composite hypothesis testing. We derive necessary and sufficient conditions on existence of a nontrivial unbiased test in the finite-dimensional Hilbert space. As a practical application, we consider the statistical hypothesis testing of entanglements. It is shown that the uniformly most powerful unbiased test is the random guess for the hypothesis testing. It implies that quantum fluctuation conflicts with the concept of hypothesis testing in classical statistics.

1 Introduction

Entanglement is the core of many wonderful applications in quantum information theory, which includes quantum teleportation [3], dense coding, and other quantum cryptographycal communications [5, 6]. Since entangled state is very fragile and likely to be affected with the external noise and interactions with the environment, various authors investigate how to validate an entanglement given experimental setup. If we have lots of sample available, state tomography is applicable, which determines each component of the density operator. As an experimentally more efficient method, entanglement witness is proposed and now used for entanglement detection [1]. Note that the entanglement witness is originally proposed as an observable which depends on a certain specific entangled state [10, 16].

Another method is given by quantum hypothesis testing (Hayashi *et al.* [9].) At least theoretically they derived the optimal testing methods in a quite restricted

situation. For example, they assume that the target state to be tested is a specific state σ (simple hypothesis). Using the LOCC protocol, the optimal test for a single entangled state is also derived [8].

However, in a more practical situation, the above assumption is too simple. For example, suppose that our purpose is to make sure that our experimental setup generates a maximally entangled state $|\Phi\rangle\langle\Phi|$, where $|\Phi\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is the Bell state. Then, their simple hypothesis is that the given state ρ is exactly the single state $|\Phi\rangle\langle\Phi|$. On the other hand, the unknown adiabatic process makes the prepared state ρ change slightly $\rho \to U\rho U^*$ while keeping the entanglement. Then, their arguments do not hold anymore even if the unitary transformation is very close to the identity. In other words, their very simple way is *not robust to the external noise.* In such a situation, we need to deal with a composite hypothesis testing. Roughly speaking, a composite hypothesis allows a certain range of the target state instead of specifying a single point.

However, as some authors pointed out, a few number of works [11, 15, 14, 4, 12] deal with composite hypothesis testing in the quantum setting. In the present paper, we focus on the unbiased test in the quantum composite hypothesis testing. We derive necessary and sufficient conditions on existence of a nontrivial unbiased test in the finite-dimensional Hilbert space. As a practical application, we consider the statistical testing of the composite null hypothesis that the prepared state is entangled against the alternative hypothesis that the state is not entangled (separable). It is shown that the uniformly most powerful unbiased test is the random guess for the hypothesis testing.

First, we briefly review quantum hypothesis testing. In Section 3, we derive theoretical result for the quantum composite hypothesis testing. Concluding remarks are given in the final section.

2 Basic setting

Now we briefly review quantum hypothesis testing. (See., e.g., Hayashi [7].) Suppose that our prepared system is represented by a density operator $\rho \in \mathcal{S}(\mathcal{H})$, where $\mathcal{H}$ is a Hilbert space and $\mathcal{S}(\mathcal{H}) := \{\rho \in \mathcal{L}(\mathcal{H}) : \mathrm{Tr}\rho = 1, \rho \geq 0\}$, where $\mathcal{L}(\mathcal{H})$ denotes linear operators on $\mathcal{H}$. Note that all of these operators are represented as matrices when we fix an orthogonal basis. As in classical hypothesis testing, we take the two hypotheses for the prepared system. Null hypothesis H_0 and alternative hypothesis H_1. If the latter holds true, it implies there happens

something significant to us. If the former holds true, nothing significant happens at all. Then we specify two disjoint subsets $\mathcal{S}_0 \cup \mathcal{S}_1 \subset \mathcal{S}(\mathcal{H})$ in order that the null hypothesis H_0 (the alternative hypothesis H_1) for a quantum state holds true if and only if $\rho \in \mathcal{S}_0$ ($\rho \in \mathcal{S}_1$). Here we assume that $\rho \in \mathcal{S}_0 \cup \mathcal{S}_1$. We identify a hypothesis $H_0(H_1)$ with a subset of density operators $\mathcal{S}_0(\mathcal{S}_1)$ below.

For example, for a bipartite system $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$, we choose a maximally entangled state $|\Phi\rangle\langle\Phi|$. Then, it is possible to consider the null hypothesis that a prepared state is very close to the entangled state $|\Phi\rangle$. It is given by

$$\mathcal{S}_0 := \{\rho \in \mathcal{S}(\mathcal{H}_{AB}) : \ \langle\Phi|\rho|\Phi\rangle \geq 1 - \epsilon\},$$

where ϵ is a fixed positive constant. Hayashi [11] deals with this kind of hypothesis testing under the assumption of group symmetry. Kumagai and Hayashi [12] deal with hypothesis testing in the quantum Gaussian states ($\mathcal{S}_0 \cup \mathcal{S}_1 \subsetneq \mathcal{S}(\mathcal{H})$).

When a hypothesis $\mathcal{S}_i, i = 0, 1$ consists of a single point, it is called a *simple hypothesis*, otherwise, called a *composite hypothesis*. Apart from theoretical interest, simple hypothesis testing, which determines whether a prepared system is ρ or σ, is less important than composite one in a practical application. However, due to technical difficulties, composite hypothesis testing has not been investigated so much.

In quantum hypothesis testing, a testing procedure is presented by one self-adjoint operator C satisfying $0 \leq C \leq I$. We call C a *test*. Given a test operator C, we perform the two-valued measurement $\{C_1 := C, C_0 := I - C\}$ for a prepared quantum state ρ. When we obtain outcome 1, we reject the null hypothesis and when we obtain the other outcome 0, we do not reject. Then we focus on the probability of the two kinds of incorrect decision. The probability of the first kind of error is given by $\alpha_\rho(C) := \mathrm{Tr}\rho C$, $\rho \in \mathcal{S}_0$ and that of the second kind of error is given by $\tilde{\beta}_\rho(C) := \mathrm{Tr}\rho(I - C)$, $\rho \in \mathcal{S}_1$. The power function of a test C is defined as $\beta_\rho(C) := \mathrm{Tr}\rho C = 1 - \tilde{\beta}_\rho(C)$. Our purpose is to reduce the probability of the second kind of error β *uniformly* for $\rho \in \mathcal{S}_1$ while keeping the probability of the first kind of error under a certain level, say, 1% or 5% (which is also called a *level of significance* and denoted as α, $0 \leq \alpha \leq 1$). If a test C satisfies $\sup\{\alpha_\rho(C) : \ \rho \in \mathcal{S}_0\} \leq \alpha$, it is called a test of level α.

Here we mention a conceptual difference between quantum state discrimination and quantum hypothesis testing, both of which are very similar mathematically. While the purpose of the former is to extract a certain information, that of the latter is to reject H_0 with keeping the probability of the false acceptance under the level α. Rejection of null hypothesis does not support the opposite hypothesis

strongly. Usually it encourages re-examination or detailed tests. (e.g. medical diagnosis, security check). Thus, quantum hypothesis testing is more suitable to validating processes in experiment or encrypted communication etc. The following definition is fundamental in the composite hypothesis testing.

Definition 2.1
A test C of significance level α is called *uniformly most powerful (UMP)* if it satisfies

$$\beta_\rho(C) \geq \beta_\rho(C'), \ \forall \rho \in \mathcal{S}_1$$

for any other test C' of level α.

Unfortunately, when all possible tests are allowed, there often does not exist any UMP test of level α in a given problem in classical statistics [13]. Situation gets worse in the quantum setting. Intuitively speaking, it is due to the unitary evolution, which does not exist in classical probability. However, when we restrict possible hypothesis testing to a smaller and reasonable class $\mathcal{C}$, it is possible to show there exists a UMP test in $\mathcal{C}$. In theoretical works, authors seem to prefer group covariance and local operation and classical communication (LOCC) so far [8, 11, 12]. In order to establish a general result of quantum composite hypothesis testing, the above condition is not so suitable. Rather, we take a weaker condition.

Definition 2.2
A test C of level α is said to be *unbiased* if the power function is greater than α,

$$\beta_\rho(C) \geq \alpha, \forall \rho \in \mathcal{S}_1.$$

An unbiased test is no less than the random decision $C = \alpha I$, which does not see the measurement outcome state at all but just guess. This random decision is called a *trivial unbiased test.*

3 Main result

3.1 Existence of nontrivial unbiased tests

In the last section, unbiased tests are defined. Our first step to understand the composite hypothesis testing in a general setting is to clarify under what conditions a nontrivial test exists. In classical statistics, in some cases there are

many nontrivial hypothesis tests and in other cases there is no such a test. There seems no simple condition. However, in quantum case, a very simple condition is derived by using a similar way to convex analysis.

Definition 3.1
Let two subsets in the quantum system $\mathcal{S}_0, \mathcal{S}_1 \subseteq \mathcal{S}(\mathcal{H})$ be nonempty and mutually disjoint. We say *the two subsets* $\mathcal{S}_0$ *and* $\mathcal{S}_1$ *are weakly separated* if there exists an nonzero self-adjoint operator X satisfying

$$\mathrm{Tr}\rho X \leq 0, \forall \rho \in \mathcal{S}_0,$$
$$\mathrm{Tr}\rho X \geq 0, \forall \rho \in \mathcal{S}_1.$$

Note that the above X is a normal vector of the separating hyperplane when we set the inner product $\langle A, B\rangle := \mathrm{Tr}A^*B$ for Hilbert-Schmidt class operators. (For separating hyperplane, see, e.g., Barvinok [2].) In finite-dimensional Hilbert spaces, a self-adjoint operator is called a *Hermitian operator*. We also note that $X = cI$, $c \in \mathbf{R}$ never satisfies the above condition because $\mathrm{Tr}\rho = 1$. Existence condition of a nontrivial test is given by the following theorem.

Theorem 3.2
Let two subsets in the finite-dimensional quantum system $\mathcal{S}_0$ *and* $\mathcal{S}_1$ *be nonempty and mutually disjoint. Suppose that either* $\rho \in \mathcal{S}_0$ *(null hypothesis) or* $\rho \in \mathcal{S}_1$ *(alternative hypothesis) holds true. Then, the following three conditions are equivalent:*

(i) Two subsets are weakly separated.

(ii) For arbitrary $0 < \alpha < 1$ *fixed, there exists a nontrivial unbiased test* T_α *for two hypotheses.*

(iii) For one $0 < \alpha < 1$ *fixed, there exists a nontrivial unbiased test* T_α *for two hypotheses.*

Proof.
First we show (i) $\Rightarrow$ (ii). Suppose that two hypotheses are weakly separated by a Hermitian operator X. Since $\dim H < \infty$, the operator norm is finite, that is, $\|X\| < \infty$ holds.

Let $0 \leq \alpha \leq 1/2$. Then, we take a test

$$C_\alpha := \frac{\alpha}{\|X\|} X + \alpha I,$$

which is not equal to the scalar times identity because $X \neq c'I$. Since $\|X\| I - X \geq 0$,

$$C_\alpha = \alpha \frac{1}{\|X\|} \{\|X\| I - X\} \geq 0$$

holds for $\alpha \geq 0$. On contrary,

$$\begin{aligned} I - C_\alpha &= (1-\alpha)I - \alpha \frac{X}{\|X\|} \\ &\geq \alpha I - \alpha \frac{X}{\|X\|} \\ &\geq 0 \end{aligned}$$

holds for $0 \leq \alpha \leq \frac{1}{2}$. For an arbitrary density operator ρ and arbitrary α, $0 \leq \alpha \leq 1$,

$$\begin{aligned} \mathrm{Tr} C_\alpha \rho - \alpha &= \mathrm{Tr}(C_\alpha - \alpha I)\rho \\ &= \alpha \frac{\mathrm{Tr} X \rho}{\|X\|} \quad \begin{cases} \leq 0, & \forall \rho \in \mathcal{S}_0 \\ \geq 0, & \forall \rho \in \mathcal{S}_1 \end{cases} \end{aligned}$$

holds. Thus, C_α satisfies the unbiasedness condition and C_α is a nontrivial unbiased test when $0 < \alpha \leq \frac{1}{2}$.

Let $\frac{1}{2} \leq \alpha \leq 1$. Then, we take a test

$$D_\alpha := (1-\alpha) \frac{X}{\|X\|} + \alpha I.$$

The test operator D_α satisfies

$$\begin{aligned} I - D_\alpha &= (1-\alpha)I - (1-\alpha)\frac{X}{\|X\|} \\ &\geq 0 \end{aligned}$$

and

$$\begin{aligned} D_\alpha &= \alpha I - (1-\alpha)\frac{X}{\|X\|} \\ &\geq (1-\alpha)I - (1-\alpha)\frac{X}{\|X\|} \\ &= (1-\alpha)\frac{1}{\|X\|}\{\|X\| I - X\} \\ &\geq 0. \end{aligned}$$

For an arbitrary density operator ρ and an arbitrary α, $0 \leq \alpha \leq 1$,

$$\begin{aligned} \mathrm{Tr}D_\alpha\rho - \alpha &= \mathrm{Tr}(D_\alpha - \alpha I)\rho \\ &= (1-\alpha)\mathrm{Tr}\frac{X}{\|X\|}\rho \\ &= (1-\alpha)\frac{\mathrm{Tr}X\rho}{\|X\|}\begin{cases} \leq 0, & \forall\rho \in \mathcal{S}_0, \\ \geq 0, & \forall\rho \in \mathcal{S}_1 \end{cases} \end{aligned}$$

holds. Thus, D_α satisfies the unbiasedness condition and D_α is a nontrivial unbiased test when $1/2 \leq \alpha < 1$.

It is trivial that (ii) $\Rightarrow$ (iii). Finally, we show that (iii) $\Rightarrow$ (i). Suppose that there exists a Hermitian operator such that

$$\begin{aligned} 0 \leq T_0 \leq I, \\ \mathrm{Tr}\rho T_0 \leq \alpha, \ \forall\rho \in \mathcal{S}_0, \\ \mathrm{Tr}\rho T_0 \geq \alpha, \ \forall\rho \in \mathcal{S}_1, \end{aligned}$$

where $0 < \alpha < 1$. We take

$$Y := \begin{cases} \frac{1}{\alpha}T_0 - I, & 0 < \alpha \leq \frac{1}{2}, \\ \frac{1}{1-\alpha}\{T_0 - \alpha I\}, & \frac{1}{2} \leq \alpha < 1. \end{cases}$$

Then, it is easily seen that two hypotheses are weakly separated by Y.
Q.E.D.

3.2 Quantum hypothesis testing of entanglement

Here we deal with the quantum hypothesis testing of entangled states. From now on, $\mathcal{S}(\mathcal{H}_A)$ is often denoted as $\mathcal{S}_A$.

Definition 3.3
Let us consider the bipartite system $\mathcal{H}_{AB} := \mathcal{H}_A \otimes \mathcal{H}_B$, where $d := \dim\mathcal{H}_A = \dim\mathcal{H}_B < \infty$. Any probabilistic mixture of product states is called a *separable state*. The remaining state is called an *entangled state*.

We set

$$\text{Sep} := \left\{ \sum_{\alpha \in A} \lambda_\alpha \omega_\alpha \otimes \sigma_\alpha \in \mathcal{S}_{AB} : \ \omega_\alpha \in \mathcal{S}_A, \sigma_\alpha \in \mathcal{S}_B, \sum_\alpha \lambda_\alpha = 1, \ \lambda_\alpha \geq 0 \right\},$$

$$\text{Ent} := \mathcal{S}_{AB} \setminus \text{Sep}.$$

Note that the summation in the definition of Sep is finite. It is due to Carathéodory's Theorem. (See, e.g., Barvinok [2] for Carathéodory's Theorem.) Clearly the subset Sep is closed and convex.

By definition, the prepared system is either an entangled state or a separable state. We consider the null hypothesis $\mathrm{H}_0 : \ \rho \in \mathcal{S}_0 := \text{Ent}$ against the alternative hypothesis $\mathrm{H}_1 : \ \rho \in \mathcal{S}_1 := \text{Sep}$. The following is the consequence of Theorem 3.2.

Theorem 3.4

Let us consider the composite hypothesis testing of H_0 against H_1. Let α denote the level of significance and $0 < \alpha < 1$. Then, there exists no unbiased test except for a trivial test $C = \alpha I$. In other words, $C = \alpha I$ is the uniformly most powerful unbiased test (UMPU test).

What the above theorem really means is that there is no way of reasonable determination of entanglement even after a single measurement. Although the statement is very simple, the proof is not so trivial. Before we prove the theorem, we need the concept of strong separation and related lemmas.

Definition 3.5

Let two subsets in the quantum system $\mathcal{S}_0$ and $\mathcal{S}_1$ be nonempty and mutually disjoint. We say $\mathcal{S}_0$ *and* $\mathcal{S}_1$ *are strongly separated* if there exists an nonzero self-adjoint operator X satisfying

$$\begin{cases} \mathrm{Tr}\rho X \leq 0, \forall \rho \in \mathcal{S}_0, \\ \mathrm{Tr}\rho X > 0, \forall \rho \in \mathcal{S}_1, \end{cases} \quad \text{or} \quad \begin{cases} \mathrm{Tr}\rho X < 0, \forall \rho \in \mathcal{S}_0, \\ \mathrm{Tr}\rho X \geq 0, \forall \rho \in \mathcal{S}_1. \end{cases}$$

In the proof of Theorem 3.4, we use Theorem 3.2, which holds under the assumption that $\dim \mathcal{H} < \infty$. However, some of lemmas below might be stated in a more general form.

Lemma 3.6

Let $\mathcal{S}(\mathcal{H})$ be the whole set of density operators ($\dim \mathcal{H} < \infty$). Let $\mathcal{S}_1$ be a nonempty closed convex subset of $\mathcal{S}(\mathcal{H})$ and $\mathcal{S}_0 := \mathcal{S}(\mathcal{H}) \setminus \mathcal{S}_1$ be a nonempty subset. Suppose that $\mathcal{S}_0$ and $\mathcal{S}_1$ are weakly separated, i.e., there exists a nonzero Hermitian operator satisfying

$$\mathrm{Tr}\rho X \leq 0, \ \forall \rho \in \mathcal{S}_0,$$
$$\mathrm{Tr}\rho X \geq 0, \ \forall \rho \in \mathcal{S}_1.$$

In addition, there exists a point $\sigma \in \mathcal{S}_1$ with $\mathrm{Tr}\sigma X > 0$. Then, $\mathcal{S}_0$ and $\mathcal{S}_1$ are strongly separated.

Proof.

It is enough to show that $\mathrm{Tr}\rho X = 0 \Rightarrow \rho \in \mathcal{S}_1$ from the assumption of the weak separation. It implies that $\mathrm{Tr}\rho X < 0, \ \forall \rho \in \mathcal{S}_0$.

Suppose that $\mathrm{Tr}\kappa X = 0$ holds for $\kappa \in \mathcal{S}_0$. We take a convex combination of this κ and σ,

$$\rho(t) := t\sigma + (1-t)\kappa \in \mathcal{S}(\mathcal{H})$$

for $0 \leq t \leq 1$. Then

$$\begin{aligned} \mathrm{Tr}\rho(t)X &= t\mathrm{Tr}\sigma X + (1-t)\mathrm{Tr}\kappa X \\ &= t\mathrm{Tr}\sigma X \end{aligned}$$

holds. When $0 < t \leq 1$, $\mathrm{Tr}\rho(t) > 0$ holds, which implies $\rho(t) \in \mathcal{S}_1$. Since $\mathcal{S}_1$ is closed,

$$\kappa = \lim_{t \to 0, t>0} \rho(t)$$

must belong to $\mathcal{S}_1$. It is contradiction. *Q.E.D.*

Lemma 3.7

Let $\mathcal{S}(\mathcal{H})$ be the whole set of density operators in the composite system $\mathcal{H} := \mathcal{H}_A \otimes \mathcal{H}_B$ ($d = \dim \mathcal{H}_A = \dim \mathcal{H}_B < \infty$). Suppose that $X \neq 0$ and $\mathrm{Tr}\rho X = 0, \ \forall \rho \in \mathrm{Sep}$ holds. Then, there exist two entangled states ρ_E and σ_E satisfying

$$\mathrm{Tr}\rho_E X > 0, \ \mathrm{Tr}\sigma_E X < 0.$$

Proof.
Since the completely mixed state I/d^2, where I is the identity operator on $\mathcal{H}$, is also separable, we obtain

$$\mathrm{Tr}\frac{I}{d^2}X = 0.$$

Thus, $\mathrm{Tr}X = 0$, which implies X has both positive eigenvalue and negative one. The corresponding normalized eigenvectors $|\psi_+\rangle$ and $|\psi_-\rangle$ are pure entangled states. (Otherwise, it contradicts the assumption.) Then,

$$\langle\psi_+|X|\psi_+\rangle = \mathrm{Tr}X|\psi_+\rangle\langle\psi_+| > 0,$$
$$\langle\psi_-|X|\psi_-\rangle = \mathrm{Tr}X|\psi_-\rangle\langle\psi_-| < 0,$$

hold. Take $\rho_E := |\psi_+\rangle\langle\psi_+|$ and $\sigma_E := |\psi_-\rangle\langle\psi_-|$. *Q.E.D.*

Now we prove Theorem 3.4 using the above lemmas.

Proof.
Due to Theorem 3.2, it is enough to show that two hypotheses are not weakly separated. Suppose that there exists a Hermitian operator $X \neq 0$ weakly separating two hypotheses.

$$\mathrm{Tr}\rho X \leq 0, \forall\rho \in \mathcal{S}_0 := \mathrm{Ent},$$
$$\mathrm{Tr}\rho X \geq 0, \forall\rho \in \mathcal{S}_1 := \mathrm{Sep}.$$

Since Sep is a closed convex subset, due to Lemma 3.6 and Lemma 3.7, X must separate strongly $\mathcal{S}_0$ and $\mathcal{S}_1$,

$$\mathrm{Tr}\rho X < 0, \forall\rho \in \mathcal{S}_0,$$
$$\mathrm{Tr}\rho X \geq 0, \forall\rho \in \mathcal{S}_1.$$

However, the set of entangled states is not a convex set. There exists a separable state σ satisfying

$$\mathrm{Tr}\rho_\alpha X < 0,\ \rho_\alpha \in \mathcal{S}_0,\ \forall\alpha \in A,$$
$$\sigma := \sum_{\alpha\in A}\lambda_\alpha\rho_\alpha \in \mathcal{S}_1,$$

where A is a finite index set and $\{\lambda_\alpha\}$ is a distribution over the set A. (e.g., take some Bell states). From the assumption of X, $\mathrm{Tr}\sigma X \geq 0$. On the other hand, the

above implies

$$\mathrm{Tr}\sigma X = \sum_{\alpha \in A} \lambda_\alpha \mathrm{Tr}\rho_\alpha X < 0,$$

which leads contradiction. *Q.E.D.*

4 Concluding Remarks

In the present paper, we consider quantum composite hypothesis testing. We obtain necessary and sufficient conditions on existence of a nontrivial unbiased test in the finite-dimensional Hilbert space. Some lemmas are derived in a similar way to convex analysis in finite-dimensional linear spaces. As a practical application, we show that the only unbiased test in the quantum hypothesis testing of the entanglement is the random guess (a trivial unbiased test). Our result implies that quantum fluctuation spoils an ordinary hypothesis testing in classical statistics. More explicit and practical methods of entanglement validation in the framework of quantum hypothesis testing will be presented in another occasion.

Acknowledgments

The author was supported by Kakenhi for Young Researchers (B) (No. 24700273). The author is also grateful to Dr. Sugiyama for fruitful discussions.

REFERENCES

[1] M. Barbieri, F. De Martini, G. Di Nepi, P. Mataloni, G. M. D'Ariano and C. Macchiavello: Detection of entanglement with polarized photons: experimental realization of an entanglement witness. *Phys. Rev. Lett.*, **91** (2003), 227901.

[2] A. Barvinok: *A Course in Convexity.* 2002, American Mathematical Society, Rhode-Island.

[3] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters: Teleporting an unknown quantum state via dual classical

and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, **70** (1993), 1895–1899.

[4] F. G. S. L. Brandão and M. B. Plenio: A generalization of quantum Stein's lemma. *Commun. Math. Phys.*, **295** (2010), 791–828.

[5] A. Ekert: Beating the code breakers. *Nature*, **358** (1992), 14–15.

[6] N. Gisin and G. Ribordy and W. Tittel and H. Zbinden: Quantum cryptography. *Rev. Mod. Phys.*, **74** (2002), 145–195.

[7] M. Hayashi: *Asymptotic Theory of Quantum Statistical Inference.* World Scientific, Singapore, 2005.

[8] M. Hayashi, K. Matsumoto and Y. Tsuda: A study of LOCC-detection of a maximally entangled state using hypothesis testing. *J. Phys. A: Math. Gen.*, **39** (2006), 14427–14446.

[9] M. Hayashi, B. S. Shi, A. Tomita, K. Matsumoto, Y. Tsuda, and Y. K. Jiang: Hypothesis testing for an entangled state produced by spontaneous parametric down-conversion. *Phys. Rev. A*, **74** (2006), 062321.

[10] M. Horodecki, P. Horodecki and R. Horodecki: Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, **223** (1996), 1–8.

[11] M. Hayashi: Group theoretical study of LOCC-detection of maximally entangled state using hypothesis testing. *New J. of Phys.*, **11** (2009), 043028.

[12] W. Kumagai and M. Hayashi: Quantum hypothesis testing for quantum Gaussian states: Quantum analogues of chi-square, t and F tests. `quant-ph/1110.6255`.

[13] E. L. Lehmann and J. P. Romano: *Testing Statistical Hypotheses.* 3rd ed., Springer, New York, 2005.

[14] M. Nathanson: Testing for a pure state with local operations and classical communication. *J. Math. Phys.*, **51** (2010), 042102.

[15] M. Owari and M. Hayashi: Local hypothesis testing between a pure bipartite state and the white noise state. `quant-ph/1006.2744`.

[16] B. M. Terhal: A family of indecomposable positive linear maps based on entangled quantum states. *Linear Algebra Appl.*, **323** (2001), 61–73.